Physical protection of lattice-Based cryptography - Challenges and solutions -

Khalid, A., O' Neill, M., Oder, T., Güneysu, T., Valencia, F., & Regazzoni, F. (2018). Physical protection of lattice-Based cryptography - Challenges and solutions -. In *GLSVLSI 2018: Proceedings of the 2018 Great Lakes Symposium on VLSI* (pp. 365-370). Association for Computing Machinery. https://doi.org/10.1145/3194554.3194616

Published in:
GLSVLSI 2018: Proceedings of the 2018 Great Lakes Symposium on VLSI

Document Version:
Peer reviewed version

Physical Protection of Lattice-Based Cryptography - Challenges and Solutions -

Ayesha Khalid
The Queen's University Belfast, United Kingdom
a.khalid@qub.ac.uk

Tobias Oder
Ruhr-Universität Bochum, Germany
tobias.oder@rub.de

Felipe Valencia
ALaRI - Università Della Svizzera Italiana, Switzerland
valena@usi.ch

Maire O' Neill
The Queen's University Belfast, United Kingdom
m.oneill@qub.ac.uk

Tim Güneysu
Ruhr-Universität Bochum & DFKI, Germany
tim.gueneysu@rub.de

Francesco Regazzoni
ALaRI - Università Della Svizzera Italiana, Switzerland
regazzoni@alari.ch

ABSTRACT

The impending realization of scalable quantum computers will have a significant impact on today's security infrastructure. With the advent of powerful quantum computers public key cryptographic schemes will become vulnerable to Shor's quantum algorithm, undermining the security current communications systems. Post-quantum (or quantum-resistant) cryptography is an active research area, endeavoring to develop novel and quantum resistant public key cryptography. Amongst the various classes of quantum-resistant cryptography schemes, lattice-based cryptography is emerging as one of the most viable options. Its efficient implementation on software and on commodity hardware has already been shown to compete and even excel the performance of current classical security public-key schemes. This work discusses the next step in terms of their practical deployment, i.e., addressing the physical security of lattice-based cryptographic implementations. We survey the state-of-the-art in terms of side channel attacks (SCA), both invasive and passive attacks, and proposed countermeasures. Although the weaknesses exposed have led to countermeasures for these schemes, the cost, practicality and effectiveness of these on multiple implementation platforms, however, remains *under-studied*.

ACM Reference Format:
Ayesha Khalid, Tobias Oder, Felipe Valencia, Maire O' Neill, Tim Güneysu, and Francesco Regazzoni. 2018. Physical Protection of Lattice-Based Cryptography - Challenges and Solutions -. In *GLSVLSI '18: 2018 Great Lakes Symposium on VLSI, May 23–25, 2018, Chicago, IL, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3194554.3194616

1 INTRODUCTION

With the societal shift towards the *Internet of Things*, ensuring security and privacy for an increasing number of heterogeneous connected devices is fast becoming a crucial concern. Moreover, our current public-key security infrastructure needs a complete overhaul since its security could be compromised by a scalable quantum computer in the near future. Quantum computers will be capable of executing Shor's algorithm which can, in polynomial time, break the two hard mathematical problems, i.e., integer factorization and discrete logarithm problem [39], on which RSA and ECC are based. These public-key schemes are used in today's security infrastructure to provide public-key encryption and (authenticated) key exchange. Reacting to this urgency, much research is now being conducted into *quantum-resilient* or *post quantum* cryptography. The concern is also reflected by the stance of government agencies, including NSA and CESG [8, 9, 25, 35]. NSA's Information Assurance Directorate (IAD) announced a transition to quantum resistant public-key cryptography in the near future for their Suite B of recommended algorithms [25]. Also, NIST announced a call requesting new quantum-resilient algorithm candidates to be considered for analysis, standardization and eventually, industry adoption [24].

Of the various flavors of quantum-resilient cryptography proposed to date, lattice-based cryptography (LBC) stands out for various reasons. *Firstly*, these schemes offer security proofs based on NP-hard problems with average-case to worst-case hardness. *Secondly*, in addition to being quantum-age secure, the LBC implementations are notable for their efficiency, primarily due to their inherent linear algebra based matrix/ vector operations on integers. *Thirdly*, LBC constructions offer extended functionality for advanced security services such as identity-based encryption (IBE) [13] attribute-based encryption (ABE) and fully-homomorphic encryption (FHE) [29], in addition to the basic classical cryptographic primitives (encryption, signatures, key exchange solutions) needed in a quantum age [16].

While LBC constructions provide security guarantees in theory, to date, the investigation of LBC implementations resilient to physical attacks remains understudied. Their realization on contemporary computing platforms requires a thorough study of their resilience, especially in the face of advanced side-channel attack techniques, both active attacks and fault attacks. This paper surveys the state of the art in physical attacks and countermeasures undertaken for LBC to date on software and hardware platforms. A significant number of attacks undertaken for non-post-quantum cryptography can be directly applicable in the LBC context, and

GLSVLSI '18, May 23–25, 2018, Chicago, IL, USA

ACM ISBN 978-1-4503-5724-1/18/05…$15.00
https://doi.org/10.1145/3194554.3194616

further vulnerabilities exposed by the inherent structures of LBC schemes need to also be investigated.

The paper is outlined as follows: Section 2 gives a background of LBC proposals and their key components. Section 3 summarizes the state of the art in physical attacks reported against LBC constructions. Section 4 discusses countermeasure proposals to date against these attacks while Section 5 concludes the paper.

2 BACKGROUND

2.1 Lattice-Based Primitives

Lattices are objects in n-dimensional Euclidean space characterized by a regular arrangement of points. More precisely, a lattice in $\mathbb{R}^n$ generated by the basis $B = \{b_1, b_2, \ldots, b_n\}$, is defined as $L(B) = \{Bx, x \in \mathbb{Z}^n\}$.

A number of hard mathematical problems are used to construct lattice-based schemes. The most commonly used problem is the Learning with Errors problem (LWE) which involves finding a vector $\mathbf{s}$ when given a matrix $\mathbf{A}$ and a vector $\mathbf{b} = \mathbf{As} + \mathbf{e}$ where $\mathbf{e}$ is a small (unknown) error vector. Other popular mathematical problems used to construct lattice-based schemes include the Short Integer Solution (SIS) or NTRU lattices.

There are three classes of lattices that are relevant for cryptography. Schemes that are based on LWE are **standard or random lattice-based schemes**. These schemes have in common that they require computations with large matrices that either need a lot of memory or require costly on-the-fly computations. A further issue with standard lattice-based schemes is that they require matrix-vector multiplication with quadratic complexity. **Ideal or ring lattice-based schemes** are an alternative to standard lattices. The major difference between these classes of lattices is that the matrix that is used in standard lattices is represented by a single row in ring lattices. The remaining rows are generated by cyclic shifts of the first row. Therefore ideal lattice-based schemes are more efficient as they require less memory and the main arithmetic operation is polynomial multiplication instead of matrix-vector multiplication. With the help of the number-theoretic transform (NTT) polynomial multiplication can be accelerated to have a complexity of $O(n \log n)$. In the case of ring lattices the security of the constructed schemes is based on ring variants of the original problems, hence, the Ring-Learning with Errors (R-LWE) or Ring-Short Integer Solution (R-SIS) are the underlying problems used in these schemes.

While ideal lattice-based schemes are more efficient, the additional structure in the lattice might also be exploitable by attacks. So far no strong attack is known that exploits the ring structure or that is better than other attacks that work on standard lattices as well. To have a trade-off between the efficiency of ideal lattices and the trust in the security of standard lattices, **module lattices** were introduced. The difference between module lattices and standard lattices is that in module lattices the matrix has small dimensions and the coefficients of the matrix are no longer simple integers but entire polynomials. Therefore the number-theoretic transform can still be used for efficient polynomial multiplication. The security of module lattice-based schemes is once again based on variants of the original mathematical problems, e.g. Module-LWE or Module-SIS.

As one of the first lattice-based cryptosystems Hoffstein, Pipher, and Silverman introduced the encryption scheme NTRU [14] in 1998 which is based on ring lattices. To date the encryption scheme NTRUEncrypt has withstood cryptanalytic scrutiny provided parameters are chosen correctly, but the NTRU-based digital signature scheme is considered broken. However, a modified version version of the signature scheme has been submitted to the NIST post-quantum call, along with many other proposals.

Table 1 presents a summary of the lattice-based schemes submitted to the NIST standardization process [24] and their related classes of lattices. Out of a total of 69 submissions to the NIST call for post quantum cryptographic proposals for digital signatures and KEM/encryption schemes, 26 are lattice-based proposals. Note that some schemes base their security on multiple assumptions. There are also two submissions based on **polynomial lattices**. This class is very similar to ring lattices and for power-of-two dimensions even equivalent. The table also shows for which key exchange (KEM)/ public key encryption (PKE) schemes the authors claim CCA or CCA2 security in addition to CPA security (which was a requirement for the NIST call). CPA security means that the scheme is mathematically secure against an attacker who has access to a limited amount of plaintext/ciphertext pairs. CCA security on the other hand implies that an attacker has access to a decryption oracle as well. This security can be extended by assuming an adaptive attacker (CCA2).

For most submitted signature schemes the authors claim EUF-CMA security, which means that a signature is existentially unforgeable under chosen-message attacks. This means that an attacker with access to a signing oracle is unable to forge a valid signature of a new message. Strong existential unforgeability under Chosen Message Attacks (SEUF-CMA) is an even stronger security notion that also assumes that an attacker is unable to forge a different signature of a message that he has already seen.

2.2 Basic Blocks for Lattice-Based Cryptography

From an architectural point of view, the key components in lattice based cryptography typically include the calculation of a series of linear algebraic operations and the sampling of values from a discrete Gaussian-distributed random source. For signatures it is beneficial to apply compression techniques (e.g., Huffman encoding) if transmission size reduction is more critical than processing cost. For ideal lattices, polynomial multiplication is typically realized using the number-theoretic transform (NTT). It is a fast Fourier transform (FFT) over a finite field where the n coefficients pass through $\log n$ *butterfly operations*. Many lattice-based cryptosystems require discrete Gaussian distribution for noise generation. In addition to the traditional *rejection sampling*, several other optimized techniques have been proposed including Bernoulli, Cumulative Distribution Table (CDT) sampling (inversion sampling), Knuth-Yao sampling, discrete Ziggurat sampling. All of these schemes have advantages depending on the target application, and hence tackling their vulnerability to side-channel attacks is critical. Random oracles needed by LBC constructions are generally instantiated by cryptographic hash functions, such as ChaCha20, SHA256, or the expandable output function (XOF) SHAKE-128.

Lattice Type	Schemes	
	KEM/PKE	Signatures
Standard	Ramstake[1] Odd Manhattan[1] LOTUS[2] Compact LWE[2] Giophantus FrodoKEM [1]	DRS
Ring, Standard	Lizard[1] Round 2[1] KCL[1] EMBELM/R. EMBELM	
Ring	NTRU Prime[2] NTRU Encrypt[2] Ding Key KINDI [1] LIMA[1] New Hope[1] HILA5 NTRU-RSS-KEM Mersenne-756839	qTESLA FALCON
Ring, Module		pqNTRUsign
Module	CRYSTALS KYBER[2] SABER [1] Three Bears [1]	CRYSTALS DILITHIUM [3]
Polynomial	Titanium [1] LAC[1]	

Table 1: Lattice based proposals submitted to NIST post quantum crytpography call

[1] IND-CCA Security
[2] IND-CCA2 Security
[3] sEUF-CMA security

3 PHYSICAL ATTACKS ON LATTICE-BASED CRYPTOGRAPHY

Physical attacks against lattice based constructions is a research direction largely unexplored. This is mainly due to the fact that lattice based constructions themselves are relatively new and several parameters of the algorithms are still under scrutiny. However, a comprehensive analysis of their resistance against physical attacks is of utmost importance for their widespread deployment. A deep understanding of the physical attack resistance of these construction is also a fundamental parameter for the NIST standardization process. In the reminder of the section, we will introduce the most common physical attacks (timing attacks, power analysis attacks, and fault attacks) and we summarize how they have been applied to lattice based constructions.

3.1 Timing Attacks

Timing attacks were first introduced by Kocher [22], they exploit the differences in time required by a device to perform specific operations, such as the non-constant time to execute two different instructions, different data fetch times due to cache memory hit/miss, programs behavior due to branching, optimizations leading to skipping of unnecessary operations, etc.

The first work discussing timing attacks on lattice-based cryptography is the one of Silverman and Whyte [40]. They mounted a timing attack an implementation of NTRUEncrypt. The attack exploits the difference in the decryption time taken by different (possibly bogus) ciphertexts since they all may require different number of calls to the hash function. To mount the attack, the adversary performs a variable number of pre-computations, and then submits a relatively small number of specially constructed ciphertexts for decryption, measuring the decryption times. Comparison of the decryption times with the precomputed data enables the attacker to recover the key in a much reduced time compared to standard attacks on NTRUEncrypt. Reported results show that for specific parameter sets, an attacker can recover a single key with approximately half of the key bits of effort. The work highlights possible ways to prevent the attack by ensuring a constant number of SHA calls. In [45], Vizev exploited the differing number of hash calls to mount timing side-channel attacks. The proposed countermeasure consists of a padding scheme, which helps ensure a constant timing of operations. A constant time sampler was also used in [6] for key-exchange in the transport layer security (TLS) protocol, based on a R-LWE implementation.

The discrete Gaussian samplers have been shown to be especially vulnerable against the timing attacks. Timing channel was exploited, where the information leaked via cache memory by a CDT based Gaussian sampler was successfully extracted [7]. To disentangle the link between timing information and the samples, Roy *et. al* proposed the use of a Fisher-Yates [11] shuffling algorithm [36, 37]. Saarinen [38] later suggested the shuffling be carried out twice on the set of independently generated samples, before summation. Recent research shows that relying solely on two-stage shuffling may not be sufficient to protect against SCA attacks [27]. Consequently, *multiple sampling and shuffling stages* together with the use of *different convolution parameters* are recommended to ensure adequate protection [27, 28].

3.2 Power Analysis Attacks

These attacks extract secret information by analyzing correlations between the un-intentional power leakage of a target device and the secret values processed during the algorithm execution. In simple power analysis (SPA), the adversary uses a limited set of power traces (possibly as few as one). One example is the single trace attack by Primas *et al.* [30] in which the authors exploit that the `DIV` instruction of an ARM Cortex-M4 microcontroller takes a varying number of cycles to finish depending on the data that is processed. The attacked implementation uses the `DIV` instruction in the modular reduction in the decryption of the R-LWE encryption scheme. The attack is able to fully recover the secret key.

The Differential power analysis (DPA) attacks are much more powerful since they collect many power traces instead to successfully suppress noise and statistically compare a single hypothetical values (*First-order DPA*) or multiple hypothetical values simultaneously (*Higher-order DPA*) with the measured power traces. In contrast to SPA, DPA targets the processed data of the implementation. Atici *et al.* presented the first power analysis attacks on NTRU in [3], targeting implementations on RFIDs. This was followed by Lee *et al.* [23], who considered first and second-order DPA attacks on NTRU. The attacks were based on the leakage of Hamming

distance information, generated during the computation of the convolution product. To prevent these attacks the authors proposed to randomize the operation order an add a random value before the computation of the convolution product (a main operation in NTRU) and subtract this value later. This countermeasure is called blinding.

In [46], Wang *et al.* considered the countermeasure proposals of [23] and suggested that blinding during the computation of the convolution products was not sufficient. A DPA was described to exploit the calculation of intermediate values. They exploit that an attacker can trigger decryptions of invalid ciphertexts. Even though illegal intermediate values would be generated, and these values would be prohibited from being output, their calculation during convolution processing stages would still be recordable in the power consumption measurements. The authors then proposed alternative countermeasures, based on random delay insertions, an alternative masking scheme and the use of dummy operations. The authors did not give any indication relating to the performance loss due to the in corporation of these countermeasures.

DPA and SPA are well understood by the community and therefore every implementation of a cryptographic scheme that does not utilize dedicated countermeasures against DPA and SPA is expected to leak secret information. The majority of the research therefore focuses on countermeasures for LBC instead of attacks against implementation of LBC.

3.3 Fault Attacks

For a fault attack the adversary purposely induces a fault and exploits the erroneous behavior of the circuit to gain information about the secret values in the cryptosystem. These errors are typically transient in nature, hence the faults *propagate through the circuit* leaving the device operating normally. The attacks are termed as *first order faults attacks* if the adversary can induce no more than a single fault in the system. The fault injection is shown to be initiated by varying the supply voltage, system clock speed or ambient temperatures, etc. [1, 2]. A further class of invasive attacks were introduced by Skorobogatov in [41, 42], with the use of destructive ion beams and semi-permanent optical fault injection techniques; the faults being shown to induce effects such as changing the values of internal registers, incorrect branching of the program or the skipping of program instructions.

A fault analysis attack against NTRUEncrypt was presented in [17] by Kamal and Youssef, where the fault model assumed the attacker is able to inject faults into the coefficients of the second step of the decryption process. Where NTRU Encrypt is implemented with parameters (N,p,q), the attack is shown to be successful with probability $\approx 1 - 1/p$. In [20], Kamal and Youssef proposed methods for strengthening hardware implementations of NTRUEncrypt against fault analysis attacks using error detection codes and duplication of the decryption operation, using a rotated version of the ciphertext in a redundant computation.

A scan based side-channel attack on NTRU Encrypt was demonstrated in [19], where the scan chain structure of the polynomial multiplication circuits was extracted, thus enabling the secret key to be retrieved. Kamal and Youssef also presented a fault analysis of the NTRU Sign digital signature scheme in [18], where it is assumed that the attacker is able to inject a transient fault into the coefficients of the polynomials in the signing algorithm. When the attacker is also able to skip the norm-bound signature check, the attack requires only one fault for success.

In [4], Bindel *et al.* investigated the vulnerability and resistance of multiple lattice-based signature schemes including BLISS, ring-TESLA and GLP signatures. They considered the first order randomizing, zeroing, and skipping faults and found effective attacks against all the signature schemes. All three schemes were found vulnerable against zeroing faults during the signing and verification, against skipping faults during the key generation, against two kinds of skipping faults during the verification. The work also suggested optimised code modifications as countermeasures against these attacks.

In [44], Valencia *et al.* discuss the vulnerability of R-LWE encryption against fault attacks. The work explored several possible fault injection effects, including single bit flip, single bit zeroing, and skip instructions and examines the consequences and the possibility of recover secret data.

In [10], Espitau *et al.* investigated the implication of early *Loop abort Faults* for various stages of lattice based signature schemes including BLISS, GLP, TESLA and the GPV scheme. For BLISS (and the rest of the Fiat-Shamir family signatures), an early termination of the generation loop for the random commitment element ($y1$) enables a full recovery of the secret key value $s1$. For GPV signature schemes too, reconstruction of the entire secret key is possible by an early loop abort fault considered for the Gaussian sample generation during signature calculation [10].

4 COUNTERMEASURES AGAINST PHYSICAL ATTACKS

This section surveys the countermeasures suggested to protect against the major physical attack vulnerabilities reported to date in LBC constructions. These countermeasures are generally device and attack specific, i.e., some custom hardware vulnerabilities and countermeasures might not be directly applicable to software implementations and vice versa. Moreover, the countermeasures may exhibit side-effects exploitable by an adversary, as shown by Regazzoni *et al.* in [31, 32] where an error detection/correction circuit may aid an adversary by increasing the available exploitable information. The automated application of power/timing attack countermeasures in gate level netlists [12, 43], that has been developed for current cryptographic schemes, is in general also applicable to lattice based circuits.

4.1 Countermeasures against Timing Attacks

The simplest countermeasure against timing attacks is to ensure that the execution time of an implementation is independent of the secret data that is processed. However, especially in the context of a Gaussian sampler, it is often expensive to have a constant-time implementation. There are several possible algorithms that utilise uniform numbers to return Gaussian distributed numbers and they differ from each other in terms of implementation speed, memory, and precision. Constant-time hardware architectures for a wide range of samplers have been proposed [15, 21]. However, to date

such proposals have been designed on a case-by-case basis and as yet there has been no proposal of a generic hardware design. The binomial sampler is inherently protected against timing attacks. However, as it only samples from a binomial distribution instead of an exact Gaussian distribution it can only be used in encryption and key exchange schemes as the security proof in signature schemes requires the sampler to have a high precision. To avoid an expensive constant-time Gaussian sampler, shuffling has also been proposed as a countermeasure [36].

4.2 Countermeasures against Power Analysis

Hiding and masking are two commonly used countermeasures against power analysis attacks. While masking tries to avoid the fact that at any point in time a secret value is stored in a register (and thus could be detected by collecting a large amount of traces), hiding uses randomization to increase the noise. While masking schemes can be provably secure as countermeasures against DPA, hiding usually makes DPA more difficult, but does not entirely prevent it. Hiding is better suited as countermeasure against SPA.

The essential goal of hiding is remove the correlation from the data computed by the device and the power consumed by the device during that computation. The most straightforward way of achieving this is to impose that an implementation must consume constant power, however, this, in practice, is extremely hard to be achieved. Another possible approach to realize hiding is to shuffle the order of the executed operations as shown in [27] and [36]. Especially for hardware implementations, it is also possible to instantiate noise generators on the FPGA or ASIC to make it more difficult for an attacker to extract the secret information from the power trace.

The idea of masking is to split the secret value into uniformly random shares and perform computations on each share individually so that an attacker needs to know every share to reconstruct the secret value. First order masking splits the secret value into two shares (i.e. with a single probe, the attacker cannot gain knowledge about the secret value).

Lee *et al.* [23] proposed three countermeasures to protect NTRU, with the aim of thwarting both first and second order attacks. The first countermeasure proposed a random initialization of every register used in the convolution operation, with the random value then subtracted after processing the final result. The second proposal was to blind the intermediate convolution steps, each with a separate random integer value. The final countermeasure was to randomize the order of the array holding the non-zero polynomials.

Masking has also been applied to R-LWE-based schemes in several works [26, 33, 34]. One obstacle when applying masking to R-LWE-based schemes is that R-LWE itself only provides security against chosen-plaintext attackers. For DPA it is essential that an attacker can trigger decryption runs on his own as DPA attacks require millions of power traces. That means that an attacker with access to a decryption oracle does not have to bother with DPA as he can simply break the cryptosystem mathematically. There are indeed use-cases where an attacker can trigger decryption runs but does not get to know the result of the decryption (i.e. DPA can be performed but not chosen-ciphertext attacks), but they are rare. Therefore it is more appropriate to apply masking to a R-LWE-based scheme that is also secure against chosen-ciphertext attackers.

Higher-order security (i.e. security against an attacker with multiple probes) can be achieved using a higher-order masking scheme. However, higher-order masking is usually expensive and therefore in practice it makes sense to combine masking with hiding as higher-order DPA attacks are very susceptible to noise in the power traces.

4.3 Countermeasures Against Fault Attacks

Errors can be intentionally introduced to a system via fault attacks, but they may also arise as a natural consequence of the mathematical constructs of the implementation, for example, calculations that have permissible error rates. When such events occur, an error recovery mechanism will detect the error and instantiate a new calculation. Hence traditional error correction codes can be used for fault error detection (and correction).

The use of the *concurrent error detection (CED)* technique has been proposed so that the normal execution of the algorithm is *suppressed* to avoid any un-intentional leakage of secret values when a fault occurs. One way of doing that is to have duplication of hardware so that in case of a mismatch of results from the two an error detection is reported. Another possibility is re-computation on the same hardware. The first approach is *resource expensive* while the second one has high *execution overhead.* In [5], various countermeasures against fault attacks for software implementations of popular lattice-based signatures are considered. Their effectiveness and overhead is evaluated for schemes including GLP, BLISS, ring-TESLA and GPV-NTRU.

5 CONCLUSIONS AND OUTLOOK

Although lattice based primitives have so far demonstrated resilience against quantum attacks, their implementation on existing commodity hardware and custom hardware will be susceptible to physical attacks. These vulnerabilities need to be addressed before LBC can be considered as a replacement for the public key cryptography suites used today. This work surveys known attacks on LBC constructions including power analysis, timing attacks and fault attacks, all of which could be a potential threat to lattice based implementations. In terms of side channel leakages, power is an important consideration. For software implementations on commodity hardware timing attack vulnerabilities are critical to address since ensuring constant timing for some algorithms, if at all possible, might result in a significant performance penalty.

Most of the countermeasures proposed to date for LBC schemes address a specific threat as they emerge (with no consideration for other threats/ countermeasures simultaneously). Typical hiding/blinding countermeasures include masking, constant time execution, randomization and fault detection. Efforts to benchmark the overhead of one or more of these countermeasures remain limited and are critical to rationalize the practicality of their adoption. There is a wealth of useful techniques to learn from traditional physical attack-resistant cryptographic designs used today but as new lattice-based designs emerge and the volume of their deployment increases, further new attacks will most likely surface and this will continue to be an important area of research going forward.

REFERENCES

[1] Ross Anderson and Markus Kuhn. 1996. Tamper resistance-a cautionary note. In *Proceedings of the second Usenix workshop on electronic commerce*, Vol. 2. 1–11.

[2] Ross Anderson and Markus Kuhn. 1997. Low cost attacks on tamper resistant devices. In *International Workshop on Security Protocols*. Springer, 125–136.

[3] AC Atici, Lejla Batina, Benedikt Gierlichs, and Ingrid Verbauwhede. 2008. Power analysis on NTRU implementations for RFIDs: First results. In *Workshop on RFID Security*. Sl: sn.

[4] Nina Bindel, Johannes Buchmann, and Juliane Krämer. 2016. Lattice-based signature schemes and their sensitivity to fault attacks. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on*. IEEE, 63–77.

[5] Nina Bindel, Juliane Krämer, and Johannes Schreiber. 2017. Hampering fault attacks against lattice-based signature schemes: countermeasures and their efficiency (special session). In *Proceedings of the Twelfth IEEE International Conference on Hardware/Software Codesign and System Synthesis Companion*. ACM, 8.

[6] Joppe W Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. 2015. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 553–570.

[7] Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, and Yuval Yarom. 2016. Flush, Gauss, and Reload–a cache attack on the BLISS lattice-based signature scheme. In *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 323–345.

[8] CESG. 2016. Quantum Key Distribution: A CESG White Paper. (February 2016). https://www.cesg.gov.uk/white-papers/quantum-key-distribution

[9] CNSS. 2015. Use of Public Standards for the Secure Sharing of Information Among National Security Systems. Committee on National Security Systems: CNSS Advisory Memorandum, Information Assurance 02-15. (July 2015).

[10] Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. 2016. Loop-abort faults on lattice-based Fiat-Shamir and hash-and-sign signatures. In *International Conference on Selected Areas in Cryptography*. Springer, 140–158.

[11] Ronald Aylmer Fisher, Frank Yates, et al. 1938. *Statistical tables for biological, agricultural and medical research*. Edinburgh.

[12] Sylvain Guilley, Philippe Hoogvorst, Yves Mathieu, and Renaud Pacalet. 2005. The backend duplication method. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 383–397.

[13] Tim Güneysu and Tobias Oder. 2017. Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things. In *18th International Symposium on Quality Electronic Design, ISQED 2017, Santa Clara, CA, USA, March 14-15, 2017*. IEEE, 319–324. https://doi.org/10.1109/ISQED.2017.7918335

[14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. 1998. NTRU: A Ring-Based Public Key Cryptosystem. In *Algorithmic Number Theory, 1998 (Lecture Notes in Computer Science)*, Joe Buhler (Ed.), Vol. 1423. Springer, 267–288. https://doi.org/10.1007/BFb0054868

[15] James Howe, Ayesha Khalid, Ciara Rafferty, Francesco Regazzoni, and Máire O'Neill. 2016. On Practical Discrete Gaussian Samplers For Lattice-Based Cryptography. *IEEE Trans. Comput.* (2016).

[16] James Howe, Thomas Pöppelmann, Máire O'Neill, Elizabeth O'Sullivan, and Tim Güneysu. 2015. Practical lattice-based digital signature schemes. *ACM Transactions on Embedded Computing Systems (TECS)* 14, 3 (2015), 41.

[17] Abdel Alim Kamal and Amr Youssef. 2011. Fault analysis of the NTRUEncrypt cryptosystem. *IEICE transactions on fundamentals of electronics, communications and computer sciences* 94, 4 (2011), 1156–1158.

[18] Abdel Alim Kamal and Amr M Youssef. 2012. Fault analysis of the NTRUSign digital signature scheme. *Cryptography and Communications* 4, 2 (2012), 131–144.

[19] Abdel Alim Kamal and Amr M Youssef. 2012. A scan-based side channel attack on the NTRUEncrypt cryptosystem. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*. IEEE, 402–409.

[20] Abdel Alim Kamal and Amr M Youssef. 2013. Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks. *Journal of Cryptographic Engineering* 3, 4 (2013), 227–240.

[21] A Khalid, J Howe, C Rafferty, and M O'Neill. 2016. Time-independent discrete Gaussian sampling for post-quantum cryptography. In *Field-Programmable Technology (FPT), 2016 International Conference on*. IEEE, 241–244.

[22] Paul C Kocher. 1996. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference*. Springer, 104–113.

[23] Mun-Kyu Lee, Jeong Eun Song, Dooho Choi, and Dong-Guk Han. 2010. Countermeasures against power analysis attacks for the NTRU public key cryptosystem. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 93, 1 (2010), 153–163.

[24] Dustin Moody. 2016. Post-Quantum Cryptography: NIST's Plan for the Future. Talk given at PQCrypto '16 Conference, 23-26 February 2016, Fukuoka, Japan. (February 2016). https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf

[25] National Security Agency. 2015. Commercial national security algorithm suite. (August 2015). https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

[26] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu. 2018. Practical CCA2-Secure and Masked Ring-LWE Implementation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018, 1 (2018), 142–174. https://doi.org/10.13154/tches.v2018.i1.142-174

[27] Peter Pessl. 2016. Analyzing the shuffling side-channel countermeasure for lattice-based signatures. In *Progress in Cryptology–INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings 17*. Springer, 153–170.

[28] Peter Pessl, Leon Groot Bruinderink, and Yuval Yarom. 2017. To BLISS-B or not to be: Attacking strongSwan's Implementation of Post-Quantum Signatures. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1843–1855.

[29] Thomas Pöppelmann, Michael Naehrig, Andrew Putnam, and Adrián Macías. 2015. Accelerating Homomorphic Evaluation on Reconfigurable Hardware. In *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings (Lecture Notes in Computer Science)*, Tim Güneysu and Helena Handschuh (Eds.), Vol. 9293. Springer, 143–163. https://doi.org/10.1007/978-3-662-48324-4_8

[30] Robert Primas, Peter Pessl, and Stefan Mangard. 2017. Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings (Lecture Notes in Computer Science)*, Wieland Fischer and Naofumi Homma (Eds.), Vol. 10529. Springer, 513–533. https://doi.org/10.1007/978-3-319-66787-4_25

[31] Francesco Regazzoni, Thomas Eisenbarth, Luca Breveglieri, Paolo Ienne, and Israel Koren. 2008. Can knowledge regarding the presence of countermeasures against fault attacks simplify power attacks on cryptographic devices?. In *Defect and Fault Tolerance of VLSI Systems, 2008. DFTVS'08. IEEE International Symposium on*. IEEE, 202–210.

[32] Francesco Regazzoni, Thomas Eisenbarth, Johann Grossschadl, and Luca Breveglieri. 2007. Power attacks resistance of cryptographic s-boxes with added error detection circuits. In *Defect and Fault-Tolerance in VLSI Systems, 2007. DFT'07. 22nd IEEE International Symposium on*. IEEE, 508–516.

[33] Oscar Reparaz, Ruan de Clercq, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. 2016. *Additively Homomorphic Ring-LWE Masking*. Springer International Publishing, Cham, 233–244.

[34] Oscar Reparaz, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. 2015. *A Masked Ring-LWE Implementation*. Springer Berlin Heidelberg, Berlin, Heidelberg, 683–702.

[35] Steven Rich and Barton Gellman. January 2014. NSA seeks to build quantum computer that could crack most types of encryption. *The Washington Post* (January 2014). https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html

[36] Sujoy Sinha Roy, Oscar Reparaz, Frederik Vercauteren, and Ingrid Verbauwhede. 2014. Compact and Side Channel Secure Discrete Gaussian Sampling. Cryptology ePrint Archive, Report 2014/591. *ePrint Report 2014/591* (2014). https://eprint.iacr.org/2014/591.

[37] Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. 2013. High Precision Discrete Gaussian Sampling on FPGAs. In *SAC*. 1–39. https://www.cosic.esat.kuleuven.be/publications/article-2372.pdf

[38] Markku-Juhani O. Saarinen. 2016. Arithmetic Coding and Blinding Countermeasures for Ring-LWE. *IACR Cryptology ePrint Archive* 2016 (2016), 276. http://eprint.iacr.org/2016/276

[39] P.W. Shor. 1994. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), .

[40] Joseph H Silverman and William Whyte. 2007. Timing attacks on NTRUEncrypt via variation in the number of hash calls. In *Cryptographers' Track at the RSA Conference*. Springer, 208–224.

[41] Sergei Petrovich Skorobogatov. 2005. *Semi-invasive attacks: a new approach to hardware security analysis*. Ph.D. Dissertation. Citeseer.

[42] Sergei P Skorobogatov and Ross J Anderson. 2002. Optical fault induction attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2–12.

[43] Mohit Tiwari, Xun Li, Hassan MG Wassel, Bita Mazloom, Shashidhar Mysore, Frederic T Chong, and Timothy Sherwood. 2010. Gate-level information-flow tracking for secure architectures. *IEEE Micro* 30, 1 (2010).

[44] Felipe Valencia, Tobias Oder, Tim Güneysu, and Francesco Regazzoni. 2018. Exploring the Vulnerability of R-LWE Encryption to Fault Attacks. *5th Workshop on Cryptography and Security in Computing Systems - Workshop - HiPEAC* (2018).

[45] Nikolay Vasilev Vizev. 2007. *Side Channel Attacks on NTRUEncrypt*. Ph.D. Dissertation. Bachelor's thesis, Technical University of Darmstadt, Germany, 2007. Available on http://www. cdc. informatik. tu-darmstadt. de/reports/reports/Nikolay_Vizev. bachelor. pdf.

[46] An Wang, Xuexin Zheng, and Zongyue Wang. 2013. Power analysis attacks and countermeasures on NTRU-based wireless body area networks. *KSII Transactions on Internet and Information Systems (TIIS)* 7, 5 (2013), 1094–1107.